NBCAD: Neighbor Based Clone Attack Detection in Cluster Based Static Wireless Sensor Networks

J.Anthoniraj[1], Dr.T.Abdul Razak[2]
[1]Research Scholar, Bharathidasan University, Trichy.
Tamil Nadu, India,
antonyrajmiet@gmail.com
[2] Associate Professor, Jamal Mohamed College, Trichy,
Tamil Nadu, India.

Abstract--Wireless Sensor Network (WSN) is a group of distributed independent sensor nodes to observe physical conditions.WSN is deployed in unattended and unsecure environment. So an adversary simply captures sensor nodes and creates clone nodes by extracting key materials. These clone nodes are deployed in the network area.WSN must be either static or mobile. In static WSN centralized and distributed protocols are available to detect clone attack. In this paper we propose a new detecting method called NBCAD to detect clone attacks in static WSN. Here sensor nodes are clustered and a Cluster Head is allocated for each cluster. In our protocol public key cryptography is used to create a link between sensor nodes and cluster. After that each node requests a session key from their cluster head for secure communication. Each node collects the neighbor node location information and stores it in a separate table. With help of the neighbor table it computes the Finger Print of the node. All messages forwarded to the cluster head must include the Finger Print of the node. The Cluster Head compares it with the existing information and identifies the clone node. The proposed protocol has significant saving of memory space, communication overhead, and ideal resilience against node compromise and achieves higher probability of detection.

Key words- Wireless Sensor Network, Clone Attack, Cluster Head, Finger Print

I. INTRODUCTION

A Wireless Sensor Network (WSN) is a distributed and self organized network. It has group of independent sensor nodes with restricted resources used to observe physical (or) environmental conditions [1].Sensor nodes are frequently called motes. The major components of a sensor node are micro controller, small memory, transceiver ,power source and one (or) more sensors. According to the applications sensor nodes are densely deployed in harsh environment [2], [3], and [4]. WSN normally consists of a Base Station that can communicate with a number of wireless sensors through a radio transceiver. Each sensor node has the capacity to collect and route data either to other sensors (or) to the Base Station directly [5], [6]. Applications of WSN include real time traffic monitoring, building safety monitoring, military sensing, heavy industrial monitoring, habitat monitoring, environmental monitoring, structural health monitoring, wildlife monitoring so on [2],[7],[8].

WSN suffers from many constraints including lack of hardware support for tamper resistance, low computation capability, very small memory, insufficient power resources, make use of insecure wireless communication channels and deployment of sensor nodes in an unattended environment these constraints make the security in WSN, a challenge[3],[9].Different possible attacks on WSN are man in the middle: attacker will be able to intercept all messages exchanging between the two victims and inject new ones. Sinkhole attack: attracting traffic to a specific node. Selective forwarding: attacker can selectively drop only certain packets. Sybil attack: node duplicates itself and presented in the multiple locations. Worm hole attack: attacker receives packets from one location of network and forwards them into another location. Flooding: attack generates large volume of traffic that prevents legitimate user from accessing services. Denial of service attack: jamming a node (or) set of nodes. Physical attack: destroy sensors permanently [9], [10], [11].

One of the physical attacks is node replication attack (or) clone attack. It is most harmful security threat to the wireless sensor networks. In this attack an adversary easily capture and compromise sensor nodes and deploy any number of clones of the compromise nodes. The replica nodes are controlled by the adversary, but have all secret keys that allow them to look like authorized participants in the network [12].The rest of this paper organized as follows. In section 2, the related work of clone attack detection methods are briefly reviewed and discussed. We describe our network model, adversary model in this paper in section 3. NBCAD protocol description is existing in section 4.The section 5 represent the experimental setup of the protocol. The section 6 describes the concluding remarks. All the notations used in the protocols are described in Table I.

TABLE I. NOTATIONS AND SIGNIFICANCE

n	Number of nodes in the network
c	Number of clusters
ngh	neighbor node
BS	Base Station
CH	Cluster Head
ni	sensor node
IDni	Identification of node ni
LCni	Location Claim of node ni
H()	Hash function
KUni, KRni	Public and private key of node ni $0 \leq i \leq n-1$
KUCHj, KRCHj	Public and private key of cluster CHj $0 \leq j \leq c-1$
KUBS, KRBS	Public and private key of Base Station BS
KSniCHj	Session key for node ni and Cluster Head CHj
KSCHjBS	Session key for Cluster Head and Base Station
KSn1n2	Session key for node n1 and node n2
m	Number of keys in a nodes key Ring
S	Key Pool

II. RELATED WORK

WSN can be either static (or) mobile. In static WSN sensor nodes do not changed their position after deployment. But in mobile WSN, sensor nodes move from their positions after deployment. In static WSN the clone attack detection categorized into centralized and distributed approach. In a centralized approach, when a new node joins the networks, it broadcast the location claim to its neighbors. One (or) more of its neighbors then forwards this location claim to the Base Station. By collecting the location information from all the nodes, Base Station can easily detect clone node, if any pair of nodes with same identity but of different locations. The drawback of this approach, if the Base Station is compromised (or) the path to the Base Station is compromised (or) the path to the Base Station is blocked; adversary can add any number of clones in the network [13],[14],[15]. The following protocols using centralized approaches to detect the clone attack.

In SET protocol all nodes in the network must have unique the intersection of any two subsets should be empty. If an adversary replicates node, the intersection of subsets including these replicated nodes will not be empty, then clone attack can be detected [16]. In New protocol each deployed node belongs to the unique group. An adversary compromising an old deployed node which belongs to an old group cannot succeed because the cloned nodes will fail to establish pair-wise keys with neighbors [17]. In CSI protocol each node broadcast a fixed number to its one hop neighbors. This fixed number can be thought of as the sensory reading of each node. If the node with the sensors reading greater that fixed number is the clone since a non clone node can only report the number once [18]. Centralized protocols have various drawbacks. The SET protocols are highly complex due to its complicated components. An adversary can misuse this protocol to revoke original nodes [16].In New protocol the sensor nodes are bound to their groups and geographic locations [17]. The following protocols using distributed approach to detect clone attack.

Distributed approach for detecting clone nodes are based on location information for a node in the network. When a new witness receives two different location claims for the same node ID, it is identified as clone node. In Broadcast protocol each node in the network uses an authenticated broadcast message to flood the network with its location information. The Broadcast protocol has high communication and memory cost for large sensor networks. The Deterministic Multicast (DM) protocol shares a node's location claim with a limited subset of deterministically chosen witness nodes. It reduces the communication cost over Broadcast protocol but selecting a fixing set of witnesses it loses resiliency. In Randomized Multicast (RM) protocol, when a node broadcast its location claim, each of the node's neighbors forwards the claim to a randomly selected set of witness nodes. It prevents the adversary from anticipating the identity of the witnesses but communication overhead equal to the Broadcast protocol[19].

In Line Selected Multicast (LSM) Protocol, when a location claim travelling from source to destination, it passes through several intermediate nodes that form claim message path. Clone node can be identified by the node on the intersection of two paths generated by two different node claims carrying the same ID and coming from two different nodes. LSM was developed as a less expensive version of RM, but it suffers from irregular distribution of witness nodes, LSM scheme reduces the communication overhead detection. The LSM protocol is similar to RM, but it has remarkable improvement in terms of detection probability [19]. Randomized Efficient and Distributed (RED) protocol Base Station broadcasts a random value to all nodes in the network. Each node broadcasts a location claim to its neighbors. The witness node selection based on a pseudo random function with the inputs of node's ID and the random value. RED has the communication overhead same as the LSM scheme. RED is more resilient in its detection capabilities than LSM. But RED protocol unable to detect masked replication attack [20].

In Single Deterministic Cell (SDC) the node broadcasts its location claim to neighbors. If a neighbor plans to forward the location claim, execute a geographic hash function to determine the destination cell. Once the location claim arrives at the destination cell, it is flooded within that cell. Parallel Multiple Probabilistic Cells (P-MPC) the location mapped and forwarded to multiple deterministic cells with various probabilities. When a node broadcast its location claim, each neighbor independently decides whether to forward the claim in the same way as in the SDC scheme. The communication over head of SDC and P-MPC will be slightly higher than RED protocol, when the network size is large. The SDC protocol flooding the first copy of a node location claim arrives at the cell and the other copies are ignored. If the first copy of location claims from the clone node, it will be distributed [15]. In Hierarchical Distributed Algorithm (HDA) Cluster Heads communicate with each other through dedicated paths and create a type of tree with Base Station as a root. The clone identification is done by the cluster nodes using a bloom filer mechanism [21]. The comparison of various static protocols described in Table II.

TABLE II. COMPARISON OF STATIC PROTOCOLS

Protocol	**Type of approach used**	**Type of Scheme used**	**Communication cost**	**Memory cost**
SET	Centralized	Base station based	$O(n)$	$O(d)$
New	Centralized	Group based	$O(\sqrt{n})$	$O(1)$
CSI	Centralized	Base station based	$O(nlogn)$	----
Broadcast	Distributed	Network broadcast	$O(n^2)$	$O(d)$
DM	Distributed	Witness based	$O(gln.g\sqrt{n}/d)$	$O(g)$
RED	Distributed	Witness based	$O(r.\sqrt{n})$	$O(r)$
RM	Distributed	Witness based	$O(n^2)$	$O(\sqrt{n})$
LSM	Distributed	Witness based	$O(n\sqrt{n})$	$O(\sqrt{n})$
SDC	Distributed	Witness based	$O(r.\sqrt{n})+O(s)$	W
P-MPC	Distributed	Witness based	$O(r.\sqrt{n})+O(s)$	W
HDA	Distributed	Cluster based	$O(N^2)$	$O(N)$
RAWL	Distributed	Witness based	$O(\sqrt{n}logn)$	$O(1)^2$
TRAWL	Distributed	Witness based	$O(\sqrt{n}logn)$	$O(n)$
DNCA	Distributed	Base station based	$O(n\sqrt{n})$	$O(n)$

In RAndomWaLk (RAWL) protocol each of the node's neighbors probabilistically forwards the claim to some randomly selected nodes. Each randomly selected node sends a message containing the claim to start a random walk on the network. The passed nodes are selected as witness nodes and it will store the claim. If any witness receives different location claims for a same node ID. This will result in the detection of the replicated node[22].will create a new entry in its trace table for recording the pass of a location claim. TRAWL reduce the memory overhead of RAWL by using a table to cache the digest of location claim. The communication overhead of RAWL, TRAWL protocols are higher than LSM [22].

Detection of Node Capture Attack (DNCA) protocol, the physically captured nodes are not present in the network during the period from the captured time to the redeployment time. The captured node can be identified by SQRT [23]. In the Cell based Identification of NOde Replication Attack (CINORA) sensor network is divided into geographical cells similar to the existing cellular network, the location claim from the nodes are distributed among a subset of cells to detect any replication[24].

III. PROTOCOL FRAME WORK

A. System and Network Model

Sensor Network has hundreds to several thousand sensor nodes. This is a static sensor network where the locations of sensor nodes do not change after deployment. This Sensor Network based on a three tiers hierarchical architecture which have sensor node, Cluster Head and Base Station. In this approach all nodes have unique pre distributed ID and deployed in a particular location. The node cannot change its location. In this architecture node send their data only to their Cluster Head whom aggregate and forward them to the Base Station. Cluster Heads create a kind of tree with the Base Station as a root. Each cluster has one Cluster Head and set of sensor nodes. The Cluster Head is more powerful in computational capability, memory storage, and life time and communication range as compared to other nodes.

Each Cluster Head knows about its member nodes in the cluster. The Base Station maintains complete topological information about Cluster Head. In the same way the Cluster Head maintains complete topological information about their member nodes. As illustrated in Table III the hardware configuration of sensor node is Berkeley mica motes called as MICAZ mote. The sensor node is equipped with an Atmel AT mega 128L processor which is based on Harvard RISC architecture. The maximum clock signal of the CPU is 8 MHz it radio receiver TICC1000 communication with data rate of 38.4 kbps at range of up to 100 feet. The standard packet size is 36 byte.

The network use the IEEE 802.15.4 Wireless Personal Area Network (WPAN) Architecture. For the Secure communication so many routing protocols are available Dynamic Source Routing (DSR) and zone routing Protocol so on. In this paper we use the GPSR (Greedy Perimeter Stateless Routing) protocol. IEEE 802.15.4 Standard defines the characteristics of the physical and MAC layers for LR-WPANS. The tasks performed by the physical layer are activation, deactivation of radio transceiver, energy detection, and channel selection so on. The MAC layer defines beacon frame, data frame are used to transferring data. The acknowledgement frame, used for confirming successful frame reception. The key management in cluster based WSNs using a hybrid technique of public keys and symmetric key cryptography. The RSA algorithm can be used for the key management. Before deployment all nodes on the cluster’s node ID, location claim are stored in the corresponding Cluster Head. All nodes in the Cluster Head load with public key of Cluster Head. A public key is pre-loaded to the sensor nodes of clusters for communication each other. A Symmetric key is assigned dynamically to Sensor nodes to establish a secure link with their neighbors.

B. Adversary Model

Adversary has the capability of capturing and compromising a limited number of legitimate nodes of the network. An adversary physically capture a sensor node, after capture the sensor node remains absent from the network for a specific period of time. It extracts all the secret materials of the captured node. After that it makes the clones of the captured node.

TABLE III. HARDWARE CONFIGURATION OF A SENSOR NODE

Parameter	Value
Node	MICA Z mote
Company	Berkely MICA mote
Processor	AT Mega 128L
Architecture	Harvard RISC architecture
Clock signal of CPU	8MHZ
Program flash memory	128KB [1000RWC]
SRAM	4KB
EEPROM	4KB-100000RWC
Radio receiver	TICC100
Radio receive data rate	38.4bps

These clones (or) replicas can be deployed in all network areas; with a single captured sensor node the adversary can create as many clones as he wants. Once clone nodes are deployed by the adversary, first try to establish secure links with their neighbors. The clone nodes are controlled by the adversary but they have key materials and look like the authorized participants of the network. So it is very much difficult to detect clone attack.

IV. NEIGHBOR BASED CLONE ATTACK DETECTION PROTOCOL

A. Public Key Management

1) Before Deployment: These clones (or) replicas can be deployed in all network areas; with a single captured sensor node the adversary can create as many clones as he wants. Once clone nodes are deployed by the adversary, first try to establish secure links with their neighbors. The clone nodes are controlled by the adversary but they have key materials and look like the authorized participants of the network. So it is very much difficult to detect clone attack.

The node ID (IDni) and location(LCni) of all the nodes in the cluster are stored in the corresponding Cluster Head. In the same way Cluster Head ID(ID_{CH})and location(LC_{CH}) of all the clusters are stored in the Base Station .The Basic Scheme picks a random pool of keys S out of total possible key space. For each node all the keys are randomly selected from the key pool S and stored into the node's memory. The set of m keys are called node's key ring.

2) Key Preloading: Master public key and corresponding master private key (KU_{BS}, KR_{BS}) are randomly selected from the key pool S and stored in the Base Station key Ring. Base Station distributes public key and corresponding private key to the Cluster Head key Ring. The public key of the Base Station also stored in Cluster Head. Public and private keys are distributed by Base Station to the nodes. Public key of the corresponding Cluster Head also stored in the node.

Step 1. $BS \rightarrow CHj$

$ID_{CHj} \,||(KU_{CHj}, KR_{CHj}) \,||KU_{BS}$

Step 2. $BS \rightarrow ni$

$ID_{ni}||(KU_{ni} ,KR_{ni})||KU_{CHj}$

3) Cluster Head Authentication: All the nodes know the public key of their Cluster Head. The Cluster Head CHj broadcast the authentication message to all its cluster nodes. This message is encrypted using the private key of the Cluster Head .Each node ni in the cluster decrypts the message using the public key of the Cluster Head and authenticates the received message.

Step 1. $CHj \rightarrow ni$

$M1=EKR_{CHj} (ID_{CHj}|| KU_{CHj})$

Step 2. ni verifies

$DKU_{CHj}(M1)$

4) Neighbor Node Discovery: Neighbor node discovery operation is performed for each of the sensor nodes in the network. The sensor nodes have limited communication range; the sensor node can only communicate with the neighbor nodes which are in its communication range.

Step 1. $n1 \rightarrow n2$

$HELLO_{Msg} (ID_{n1}, ID_{CH1})$

Step 2. $n2 \rightarrow n1$

$HELLO_{Msg} (ID_{n2}, ID_{CH1})$

Step 3. $n1 \rightarrow n2$

$HELLO_{Msg} (KU_{n1}, || ID_{n1})$

Step 4. $n2 \rightarrow n1$

$M2=EKU_{n1}(HELLO_{Msg} (ID_{n2}))$

Step 5. n1 verifies

$DKR_{n1}(M2)$

The neighbor node discovery can be performed by transmitting the HELLO message. Node n1 broadcast HELLO message to all its neighbor nodes along with its ID and ID of cluster Head. Those nodes who receive this HELLO message are in the communication range of node n1. Node n2 is in the communication range of node n1, so it receives HELLO message sent by node n1. After that n2 will send the HELLO message to n1 along with its ID and ID of cluster Head .Now node n1 distribute the public key to node n2. Node n2 acknowledges the node n1 by sending its ID by encrypt with the public key of n1. Node n1 decrypt the reply message and verified it.

B. Session Key Establishment

1) Session key Establishment with neighbor nodes: Here we establish a symmetric communication between all the neighbor nodes of a particular node. After receiving the reply message for public key distribution, node n1 send the session key to node n2. Node n2 receive the session key and send the reply message to n1.

Step 1. n1 → n2
$M3= EKR_{n1} (ID_{n1}, KS_{n1n2})$

Step 2. n2 verifies
$DKU_{n1} (M3)$

Step 3. n2 → n1
$KS_{n1n2} (ID_{n1}, ID_{n2})$

2) Node Seeking Admission With the Cluster Head: In order to communicate with Cluster Head all nodes in the cluster must get admission with the Cluster Head. Node n1 send the admit request to Cluster Head CH1 along with its location claim.

Step 1. n1 → CH1
$M4= EKU_{CH1}(admitReq,ID_{n1},ID_{CH1},LC_{n1})$

Step 2. CH1 verifies
$DKR_{CH1} (M4)$

Step 3. If existing $[ID_{n1},LC_{n1}] = $ received$[ID_{n1},LC_{n1}]$
Node Admission accepted

Step 4. CH1→ n1
$M5= KR_{CH1}(admitAccept,ID_{n1},ID_{CH1},KS_{CH1n1})$

Step 5. n1 verifies
$DKU_{CH1}(M5)$

Step 6. n1→CH1
$KS_{n1CH1}(sesKeyAccept,ID_{n1}, ID_{CH1})$

Step 7. If existing $[ID_{n1},LC_{n1}] \neq$ received$[ID_{n1},LC_{n1}]$
Clone node identified

Now Cluster Head CH1 receive the admission request from the node n1 and compare ID_{n1},LC_{n1} received with the existing information. If existing information (ID_{n1},LC_{n1}) stored in the CH1 match with the received information then CH1 send the admit Accept message to the node n1.Along with, it also send the session key for secure communication between node n1 and Cluster Head. When node n1 receive the session key it decrypt it using the public key of the Cluster Head and send reply message to the Cluster Head. If existing information (ID_{n1},LCn1) stored in the CH1does not match with the received information then node n1 is identified as a clone node. Likewise all nodes seek admission with their Cluster Head, the Cluster Head verify the admission request and provide the session key to that node.

3) Cluster Head Seeking Admission with the Base Station: In order to communicate with Base Station the entire Cluster Heads must get admission with the Base Station. Cluster Head CH1 send the admit request to the Base Station BS along with its location claim. Now Base Station decrypt the message with private key of Base Station and compare ID_{n1},LC_{n1} received with the existing information. If existing information (ID_{n1},LCn1) stored in the BS match with the received information then BS send the admit Accept message to the Cluster head CH1. Along with, it also send the session key for secure communication between Cluster Head CH1 and BS. When CH1 receive the session key it decrypt it using the public key of the BS and send reply message to the Base station BS. Likewise all Cluster Heads seek admission with Base Station, the base station verify the admission request and provide the session key to that Cluster Heads.

Step 1. CH1→ BS
$M6= KU_{BS}(admitReq,ID_{BS},ID_{CH1},LC_{CH1})$

Step 2. BS verifies.
$DKR_{BS}(M6)$

Step 3. If existing$[ID_{CH1},LC_{CH1}] = $ received$[ID_{CH1},LC_{CH1}]$
Admission accepted

Step 4. BS→ CH1

$M7= EKR_{BS}(admitAccept,ID_{BS},ID_{CH1},KS_{BSCH1})$

Step 5. CH1 verifies

$DKR_{BS}(M7)$

Step 6. CH1→ BS

$KS_{BSCH1}(sesKeyAccept,ID_{BS}, ID_{CH1})$

Step 7. If existing $[ID_{CH1},LC_{CH1}] \neq$ received$[ID_{CH1},LC_{CH1}]$

Clone node identified

4) Collecting Location Claim of the Neighbor Nodes: Node n1 send the location information request to the node n2. Node n2 decrypt the received message with the session key and send the location information to n1 by encrypting this information with the session key along with the signature. Node n1 receive the message and verified the signature. Decrypt the message with the session key, decrypt the signature with public key of node n2 and store the node ID and location claim in the neighbor table described in Table IV.

Step 1. n1→n2

$M8=EKS_{n1n2}(LocInfReq,ID_{n1},ID_{n2})$

Step 2. n2 verifies

$DKS_{n1n2}(M8)$

Step 3. n2→n1

$M9=EKS_{n1n2}(LocInf,ID_{n2},LC_{n2}(EKR_{n2}(H(ID_{n2},LC_{n2}))))$

Step 4. n1 verifies

$DKS_{n1n2}(M9)$

Step 5. Store the location claim in the neighbor table

TABLE IV. NEIGHBOR TABLE

Node ID (ID_{ni})	**Location Claim (LC_{ni})**
…. ….	…. ….

Likewise n1 collect the node ID and Location claim of all its neighbor nodes and store this information in the neighbor table.

D. Clone Node Verification

The Cluster Head has the node ID and Location claim of all the nodes in its cluster. Node n1 send its entire neighbor node List to the Cluster Head for verification. The Cluster Head (CH1) verifies the node ID and its Location claim with the already existing Information. If any node has correct node ID but different Location claim for a particular node means, it is identified as the clone node.

Step 1. n1→CH1

$M10=ERS_{n1CH1}$ (ClCheck,<nghID List > <nghLCList>)

Step 2. CH1 verifies

$DRS_{n1CH1}(M10)$

Step 3. CH1→n1

$M11 = ERS_{n1CH1}$ (CloneFind,<Clone node list >)

Step 4. n1 verifies

$DRS_{n1CH1}(M11)$

The Cluster Head identified all the clone nodes in the List and sends the list of clone nodes in the neighbor node List given by the node n1. CH1 computes the Finger Print for node n1 with help of the neighbor node list. The n1 receive the clone node List from the Cluster Head and remove all the clone nodes from the neighbor table.

E. Clone Node Detection using the Finger Print

The node n1 send all its neighbor List to the Cluster Head, it verify the nodes and give the clone node List to node n1 according to that node n1 remove all clone nodes and prepare new neighbor node List. With help of the new neighbor node List the finger print of the node n1 is compute with the Boolean sum of the neighbor node IDs. Node n1 send any content to the cluster head it should attach the finger print FP_{n1} with the message.

```
Step 1.   Compute the Finger Print
          $FP_{n1}$ = ngh1 (ID) V ngh2 (ID) V ngh3 (ID))
Step 2.   n1→CH1
          $EKS_{n1CH1}$(cont, $ID_{n1}$, $FP_{n1}$ ($EKU_{CH1}$(H ($ID_{n1}$, $FP_{n1}$))))
Step 3.   If Existing[$ID_{n1}$, $FP_{n1}$] = Received[$ID_{n1}$, $FP_{n1}$]
          Node content accepted
Step 4.   If Existing[$ID_{n1}$, $FP_{n1}$] ≠ Received[$ID_{n1}$, $FP_{n1}$]
          Clone node identified.
```

The cluster already computes the Finger Print of all the nodes with help of the updated neighbor node List of that node. FP_{n1} of node n1 also stored in the memory of the Cluster Head CH1When node n1 send any message to cluster Heads CH1, first decrypt the message and verified the signature. Now compare the FP_{n1} given in the message with existing FP_{n1} of the node n1, if both are same the content of the node n1 is accepted. If the FP_{n1} given by the node n1 is not match with the existing FP_{n1}, then is node is identified as the clone node. The clone node Identification is informed to the Base Station and all other nodes in the Cluster Head.

V. EXPERIMENTAL SETUP

Visual Studio and Qual Net NetSimCap is used as simulation tool to implement our protocol. In our experiment we construct a static sensor network with 100 sensor nodes, it have 10 clusters and each cluster have 10 sensor nodes, The various simulation parameters used in the experiment are described in Table V. The protocol is loaded using VC++ programming interface component NETSIMCAP. NETSIMCAP uses the function NC::Load User Defined MOTE Protocol(file, pch file, auto complete);The parameters used (1)file - Document File. (2)pch file – Precompiled version of Document File.(3)auto complete=1(always).

TABLE V. SIMULATION PARAMETERS

Parameter	Value
Surface of the network	$1000m^2$
Total no-of Nodes	100
Number of clusters	10
Number of nodes in the cluster	10
Size of data packet	512 B
Routing Protocol	GPSR
Channel Bandwidth	20 Kpbs
Architecture	IEEE.802.15.4 LR-WPAN Zigbee
Transmission radius	50m
Raw Data Rate	868 MHZ:20 kp/s
Channels	868/915 MHZ :11 Channels 2.4GHZ : 16 Channels

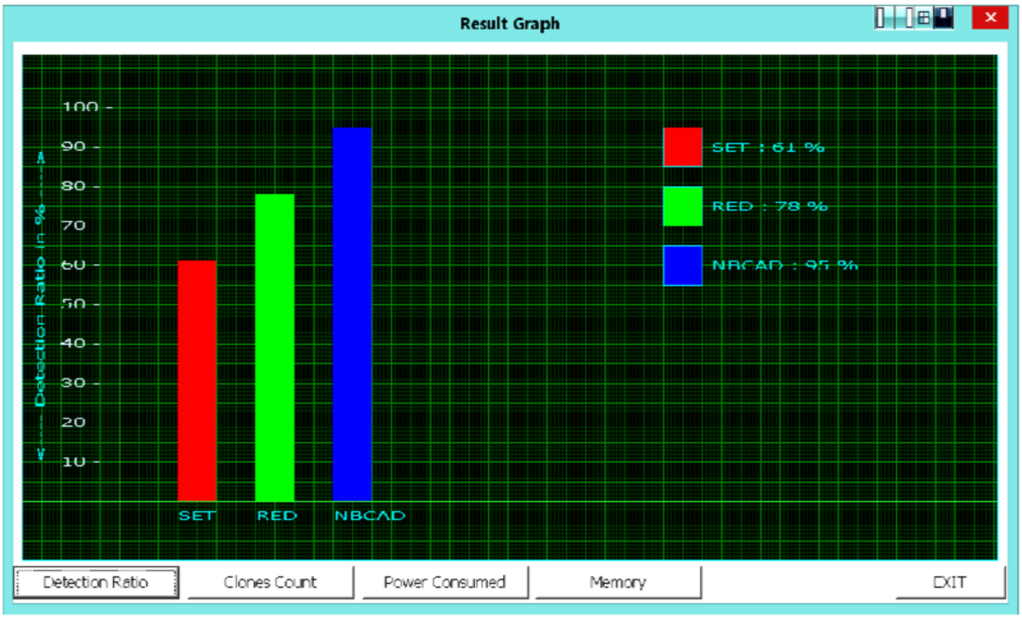

Fig 1. Comparison of Detection ratio with SET and RED protocols

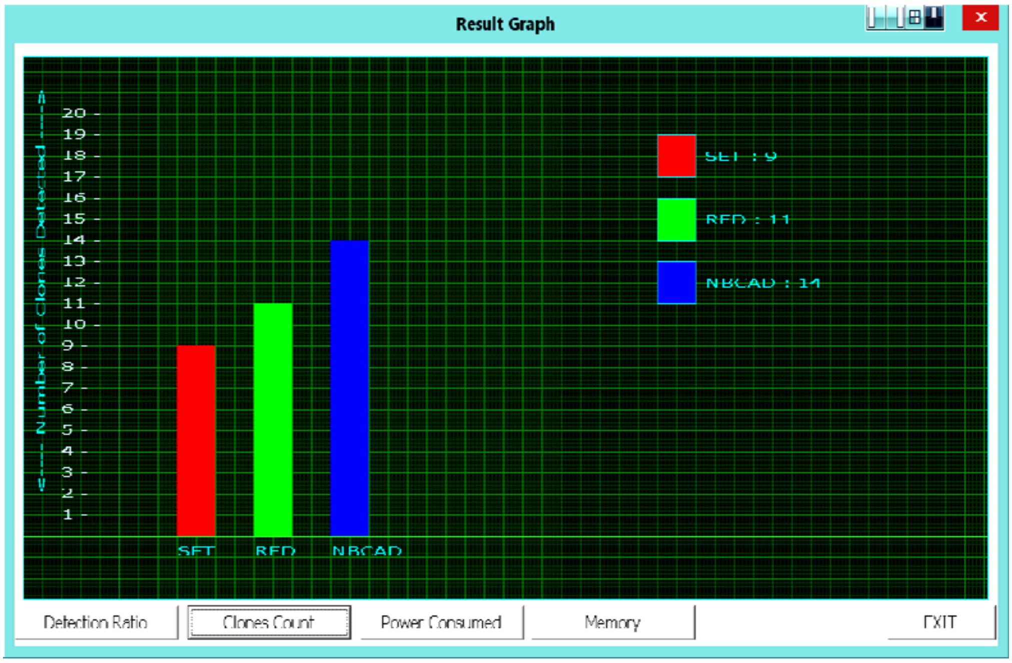

Fig 2.Comparison of Total number of clones detected in SET and RED protocols

Fig. 1 shows the comparison of detection ratio of NBCAD protocol with SET and RED protocols. The SET protocol give the 61% detection ratio, RED protocol have the 78%,but our NBCAD protocol have 96% detection ratio. This result shows NBCAD protocol has more detection ratio than other protocols. The fig.2 shows how many no of clones are detected in various protocols. In our experiment 100 sensor nodes are deployed in the field and 20 clone nodes try to enter in to the network. The SET protocol detect 9 clone nodes, RED protocol detect 11 clone nodes, but our NBCAD protocol detect 14 clone nodes. So compare with SET,RED protocols NBCAD protocol detect more number of clone nodes.

VI. CONCLUSION

In this paper we propose a Neighbor Based Clone Attack Detection (NBCAD) Protocol for detecting clone nodes in static sensor networks. We have presented a key management scheme for clustered WSNs which use both public and symmetric key cryptography. In our scheme each node communicates with the neighbor nodes and cluster head. This will reduce the transmission range and power consumption of the nodes. NBCAD protocol use very minimum power consumption than RED protocol. Our protocol use less memory space than SET and RED protocols. NBCAD provides more security and higher probability of clone detection than SET and RED protocols.

REFERENCES

[1] T.Bonact, P.Lee, L.Bushnell and R.Poovendra “Distributed clone detection in wireless sensor networks : an optimization approach” in proceeding of 2nd IEEE International workshop on data security and privacy in wireless networks, Italy, June 2011.

[2] Christoph Kraub, “Handling insider attacks in Wireless Sensor Networks”,Ph.D Thesis, Technische University,Darmstadt,2010.

[3] Yong Wang, Garban Attebury and B. Ramamurthy, “A Survey of security issues in Wireless Sensor Networks”, IEEE Comm. Survey and Tutorials, Vol.8,No.2,2nd Quarter 2006.

[4] IanF. Akyildiz, Weillian Su, Y. S.Subramaniam and Erdal Cayifici, “A Survey on Sensor Networks ”, IEEE Comm. Magazine, pp 102-114,August 2002.

[5] Cris Townsend, S.Arms, Wireless sensor networks Principles and applications, Sensor Technology Handbook, Elsevier Inc.2005,Chapter 22, pp 439-449.

[6] JamalN.AL-Karaki, Ahamed E.Kamal, “Routing techniques in Wireless sensor networks: A Survey”, IEEE Wireless Communications, December 2004.

[7] Haowen Chan,Adrian Perrig,Dawn Song, “Random key Pre distribution schemes for sensor networks” in proceeding of IEEE Symposium on Security and Privacy,2003.

[8] Y.Yu, V.K.Prasanna, B.Krishnamachari, “Information processing and routing in wireless sensor Networks” ,World scientific Publications,Dec-2006.

[9] Dr.G.Padmavathi, Mrs Shanmuga Priya, “A Survey of Attacks Security mechanisms and Challenges in Wireless Sensor Networks”, ,International Journal of Computer Science And Information Security, Vol.4,No.1&2,2009.

[10] Rishav Dubey, Vikram Jain, Rohit Singh Thakur, Siddharth Dutt Choubey , “Attacks in wireless sensor networks”, International Journal of Scientific and engineering research, Vol 3,Issue 3,March 2012.

[11] M. Sharifnejad, M. Sharifi, M.Ghiasabadi, S. Beheshti, “A Survey on Wireless Sensor Networks Security”,4thInternational conf. on Science of Electronic technologies of Information and Telecommunications, March 2007.

[12] P.mohanty, S.Panigrahi, N.Sarma and S.Sankar Satapathy “Security issues in Wireless Sensor Network Data Gathering Protocols: A survey”, Journal of Theoretical and Applied Information Technology,pp.14-29, 2010.

[13] D.Sheela, Priyadarshini, Dr.G.Mahadevan, “ Efficient To detect clone attacks in wireless sensor networks”, IEEE Communications,2011.

[14] Bo Zhu,V.G.Krishna Addada,Sanjeev Setia,Sushil Jajodia, Sankardas Roy, “Efficient distributed detection of node Replication attacks in wireless sensor networks”, 23rd Annual computer security applications conference, IEEE Computer society,2007.

[15] B.Zhu, S.Satia, S.Jajodia, S.Roy, L.Wang, “Localized Multicast: Efficient and Distributed Replica Detection in large Scale Sensor Networks”, IEEE Transactions On Mobile Computing, Vol.9, No.7, pp.913-926, July 2010.

[16] H.Choi, S. Zhu, T.F.L. Porta, “SET: Detecting node clones in Sensor Networks”, Proc of 3rd International Conference on Security and Privacy in Communication Networks, pp 341-350, Sept 2007.

[17] C.Bekara and M.Laurent Maknavicius, “A new protocol for securing wireless sensor networks against nodes Replication attacks” , 3rd IEEE International Conference on Security and privacy in communication networks,2008.

[18] C.M.Yu, C.S.Lu and S.Y.Kuo, “CSI: Compressed sensing Based clone identification in sensor networks” ,Proc of the IEEE International conference on pervasive computing And Communications Workshops ,pp 290-295,March-2012

[19] B.Parno, A.Perrig,V.Gligor, “Distributed Detection of Node Replication Attacks in Sensor Networks” ,In proceeding of the IEEE symposium on Security and Privacy,2005.

[20] M. Conti, R. Di Pietro, L.V.Mancini and A.Mei, “A Randomized, efficient and Distributed Protocol for the Detection Of Node Replication Attacks in Wireless Sensor Networks” ,Proc.ACM Mobi Ad Hoc Networking and computing, pp 80-89,Sept 2007.

[21] W. Znaidi, M. Minjer,S. Ubeda, “Hierarchical Node replication Attacks Detection in Wireless Sensors Networks” , IEEE Communications ,pp 82-86,2009.

[22] Y. Zeng, J. Gao, S.Zhang, S. Gao And L. Xie, “Random Walk Based Approach to Detect Clone Attacks in Wireless Sensor Networks”, IEEE Journal on Selected areas in Communications, Vol 28,No.5,pp 677-691,June 2010.

[23] J.W. Ho, “Distributed detection of node capture attack in Wireless sensor networks ”, in smart wireless sensor Networks ,pp 345-360,InTech,Croatia,2010.

[24] S.Gautam Thakur, “ CINORA: Cell based identification of Node Replication Attacks in wireless sensor networks”, in Proceedings of the IEEE International Conference on Communications Systems,2008.